anand guru

SOC EXPERTS

Interview Questions on
Vulnerability Management

Anand Guru

Security+ | CySA | CEH | ECIH

Founder

SOC Experts

https://socexperts.com

What is Vulnerability?

- A vulnerability is a weakness in a system, network or application.
  - System – Running with older version of a software
  - Network – Use of unsecure protocols
  - Application – No user input validation (leads to injection attacks)

What is Threat?

- Anything/Anyone that can exploit a vulnerability, intentionally or accidentally is a Threat

  Example: An attacker or Earthquake or Untrained Staff

What is Risk?

- The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability.

  Example: Financial losses because a e-commerce server is down, Loss of reputation etc.

What is Exploit?

- A tool used to take advantage of the vulnerability.

  Example: Eternal Blue (take advantage of SMB vulnerability)

anand guru

What is Vulnerability Assessment?

- Vulnerability Assessment is the process of defining, identifying, classifying and prioritizing vulnerabilities in computer systems, applications and network infrastructures.
- Vulnerability Assessment team closely works with other infrastructure teams to help them remediate/patch vulnerabilities with the systems they manage.

anand guru

Explain Vulnerability Management life cycle.

- **Discover** - Discover all the assets (using an host discovery scan)
- **Prioritize Assets** - Prioritize the assets based on the criticality and risk.
- **Assess** - Perform Vulnerability Assessment to identify vulnerabilities
- **Report** - Report all the vulnerabilities, based on criticality and business risk
- **Remediate** - Remediate the vulnerabilities by applying the patches or modifying the configurations
- **Verify** - Confirm that the patch has be applied successfully by rescanning the machines

anand guru

What is the difference between VA and Penetration Testing?

- Vulnerability Assessment is all about identifying the vulnerabilities and reporting them for patching and remediation.
- Penetration Testing is going one step ahead (after identifying the vulnerabilities) and exploiting the vulnerability.
- Penetration Testing will help companies assess the risk in a better way.

anand guru

Name few VA tools?

- The popular Vulnerability Assessment tools are
  - ✓ Tenable Nessus
  - ✓ Qualys Guard
  - ✓ Rapid7 Nexpose
  - ✓ OpenVAS (Open Vulnerability Scanner) – Open source tool

anand guru

What is a Scan Template?

- A scan template is a pre-configured setting for a specific type of scan a user wants to perform.

  Example:

  - Advance Scan
  - Host Discovery Scan
  - PCI Compliance Scan
  - Specific Vulnerability Scan (Scan for WannaCry Ransomware)

Scan Templates
Back to Scans
NESSUS Scan Templates
Scanner
User Defined
DISCOVERY
Host Discovery
A simple scan to discover live hosts and open ports.
VULNERABILITIES
Basic Network Scan
A full system scan suitable for any host.
Advanced Scan
Configure a scan without using any recommendations.
Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.
Malware Scan
Scan for malware on Windows and Unix systems.
UPGRADE
Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.
Web Application Tests
Scan for published and unknown web vulnerabilities.
Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.
Badlock Detection
Remote and local checks for CVE-2016-2118 and CVE-2016-0128.
Bash Shellshock Detection
Remote and local checks for CVE-2014-6271 and CVE-2014-7169.
DROWN Detection
Remote checks for CVE-2016-0800.
Intel AMT Security Bypass
Shadow Brokers Scan
Spectre and Meltdown
WannaCry Ransomware

anand guru

How do VA Scanner identify Vulnerabilities?

- Most VA scanners use some kind of Scripting languages to scan the machines and the results are compared with the database of know vulnerabilities.
- A vulnerability scanner can also detect weak configurations and passwords, no password, default passwords.
- Some of the scripts looks for Registry values to identify the version and patch level of an application.

anand guru

Where do you find Vulnerability details?

- Few good source of all the vulnerabilities are
  - www.cvedetails.com
  - www.nvd.nist.gov (National Vulnerability Database)
  - www.cve-mitre.org

What is CVE?

- CVE stands for Common Vulnerabilities and Exploits. It is a number given to each identified vulnerability.
- CVE is a list of entries—each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities.
- The format of the CVE is:

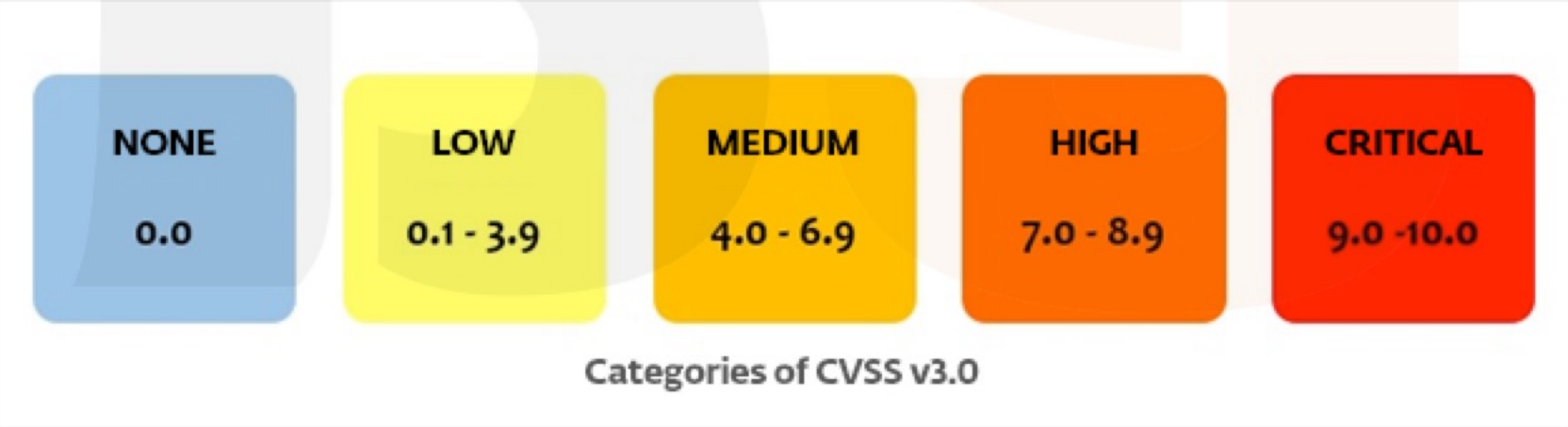
  CVE prefix + Year + 4 Arbitrary Digits (CVE-YYYY-NNNN)

  Example: **CVE-2019-1760**

anand guru

What is CVSS?

- CVSS stands for Common Vulnerability Scoring System. It is an industry standard used by vendors to define the criticality of a vulnerability. The score ranges from 0 to 10.
- CVSS are categorized as below:



Categories of CVSS v3.0

How frequently should a Vulnerability scans be run?

When does a company run Vulnerability Scans?

- Vulnerability assessments are usually performed on a scheduled basis, typically Monthly once or Quarterly once.
- Also scan can be run on need basis. A solid example is when a new headline vulnerability emerges. When this vulnerability assessment is performed, the scan are configured to specifically look for the new vulnerability.

What is Patch Management?

- **Patch management** is the process of applying (installing) patches to a system or application in order to get new features, fix bugs or security issues.

Difference between Hotfix, Patch and Service Packs.

- **Hotfix** addresses only one bug(issue). Typically does not require a reboot.

  v8.5.0 to 8.5.0 Build 20200101

- **Patch** is a collection of hotfixes and new features. Usually requires a reboot of the system to be effectively applied.

  v8.5.0 to 8.5.1

- **Service Pack** is collection of patches.

anand guru

What is Change Management?

- Change management is the process, tools and techniques to manage the people side of change to achieve the required business outcome.
- Change management helps in reducing the risk associated with the change.
- When a team (or individual) wants to perform a change in the server, they raise a Change Request (CR)

Change Request Form Template			
Project Name	Name of project		
Requested By	Name of requestor	Date	Date request was raised
Request No	Request Number	Name of Request	Brief name of request
Change Description	Description of the change		
Change Reason	Give the justification for the change		
Impact of change	Specify the impact of the change in terms of cost impact, budget impact, schedule impact, and impact on other projects.		
Proposed Action	Does the project manager propose this change is accepted/rejected and why		
Status	In review	Approved	Rejected
Approval Date	The date the change was approved or rejected		
Approved By	Who approved the change (usually the project manager or project sponsor)		

What is Buffer Overflow Vulnerability?

- Buffer Overflow vulnerability is a weakness in an application that lets an attacker over-run the fixed length block of memory. It is possible that attacker might consume the entire memory there by slowing down or crashing the server. This leads to Denial of Service attack.

  Example: CVE-2016-6808 - Buffer overflow in Apache Tomcat Connectors (mod_jk) before 1.2.42.

What is Remote Code Execution Vulnerability?

- Remote Code Evaluation is a vulnerability that when exploited gives the attacker execute commands on the compromised server.
- A Remote Code Evaluation can lead to a full compromise of the server.

Example: CVE-2019-1238 - VBScript Remote Code Execution Vulnerability

If a vulnerability cannot be patched immediately, what has to be done?

- Step up the security for the server
  - Like Tighten the configurations on OS, AV, Host Firewall etc.
- Check with IPS team if there is a signature available to detected if the vulnerability is being exploited, if so assign a high severity to it
- Increasing the level of monitoring on the server.
  - Typically done by putting the affected server(s) in a list and writing more sensitive rules.
  - Like if the default threshold for Brute-force is 100 attempts in 1 minute. On this server it will be 10 in 1 minute.

What are the vulnerabilities you have worked on?

- I can always recall working on the WannaCry Ransomware Threat.
- The weakness (vulnerability) was with Microsoft's SMBv1 **(MS17-010)**
- Microsoft had already released the patch.
- We had 800 Windows Servers and around 4000 Windows Client Machines.
- We were working closely with server/system team and vulnerability management team.
- Scans were scheduled almost hourly basis on different network segments.
- Pulling reports on a regular basis. We presented a report to our CISO every 3 hours once for almost 4 days. Till we got 98% of the machines patched.

What is the latest vulnerability you have heard of?

- Look at the latest vulnerability
- Get the Vendor, Product and Version of product it is present in.
- Try to remember the CVE number if possible.
- Understand how the vulnerability can be exploited.
- Check if a patch is already available.
- See if any major attacks have happened because of this vulnerability.
- Try to relate the vulnerability to your organization.
  - Did it affect the company you are working with?
  - How did you company handle the vulnerability?
  - What teams were involved in patching?

Full course on Udemy

IT & Software › Network & Security › Cyber Security

SOC Analyst (Cybersecurity) Interview Questions and Answers

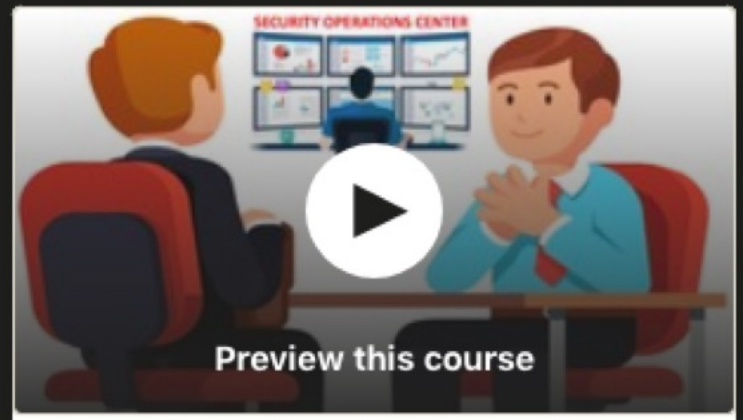
Clear your next SOC interview with ease with these 300+ interview question asked during most SOC Analyst Interview

Bestseller 4.6 ★★★★½ (106 ratings) 2,248 students

Created by Anand Guru

Last updated 5/2020 English English

Wishlist Share Gift this course



₹455 ~~₹1,280~~ 64% off

5 hours left at this price!

Add to cart

Buy now

30-Day Money-Back Guarantee

What you'll learn

- ✓ Security Analyst/SOC Analyst interview questions and how to answer them
- ✓ Tricky questions and how to answer them
- ✓ Scenario based questions
- ✓ SOC Analyst Training
- ✓ Wide range of topics covered in a SOC Interview
- ✓ How to answer experience related questions
- ✓ Ready-to-use sample CVs for SOC Analyst role

This course includes:

- 2.5 hours on-demand video
- 2 articles
- 8 downloadable resources
- Full lifetime access
- Access on mobile and TV
- Certificate of completion